IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	)))	MDL No. 1:19md2915 (AJT/JFA) JURY TRIAL DEMANDED

This Document Relates to the Consumer Cases

PLAINTIFFS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION FOR CLASS CERTIFICATION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

INTRODUCTION

Proposed Class Representatives Emily Behar, Brandi Edmondson, Emily Gershen, Brandon Hausauer, Sara Sharp, John Spacek, Caralyn Tada, and Gary Zielicke, respectfully submit this memorandum of law in support of their motion under Rules 23(a), 23(b)(3), 23(b)(2), 23(c)(4), and 23(g) to certify this action as a class action, certify the proposed classes as defined below, appoint Class Representatives for the proposed classes, and appoint Karen Hanson Riebel, Norman E. Siegel, and John A. Yanchunis as Class Counsel and Steven T. Webster as Liaison Counsel for the classes.

This MDL arises from a massive data breach announced by Capital One on July 29, 2019, affecting approximately 98 million Americans who were applicants for Capital One credit cards (the "Breach"). As set forth below, exhaustive fact and expert discovery establishes by a preponderance of the evidence that the elements of Rule 23 are satisfied and the class claims should therefore be certified for trial. The evidence supporting certification includes voluminous evidence of Capital One's and AWS's[1] catastrophic failures in protecting the sensitive personally identifiable information ("PII") they were duty bound to protect, and Capital One's breaches of its promises regarding security of PII made to the bank's credit applicants. This case is well suited to class resolution because the central common questions—e.g., whether Capital One and AWS had an obligation to secure the PII at issue, whether they failed to meet their obligations through lax data security, and whether their security failings caused the exfiltration of the PII—will be

[1] The Capital One Defendants include Capital One Financial Corporation, Capital One Bank (USA) N.A., and Capital One, N.A. and will be referred to collectively as "Capital One." The Amazon Defendants include Amazon.com, Inc. and Amazon Web Services, Inc. and will be referred to collectively as "AWS." All defendants together shall be referred to as "Defendants."

answered through common evidence of the Defendants' conduct, without regard to any potential differences among class members.

In addition to class-wide common evidence focusing on Capital One's and AWS's negligent and otherwise actionable conduct, the Proposed Class Representatives' testimony supports their claims of class membership, injury typical of other class members, and adequacy in representing absent class members. Moreover, five highly-qualified experts support the notion that common issues far predominate over individual ones, and opine on appropriate damages methodologies that can be applied across the classes.

Finally, a class action is the superior method—indeed, the only practicable method—to adjudicate the claims and remedy the wrongs at issue in this case. Thus, as discussed further below, Plaintiffs' motion should be granted.

FACTUAL BACKGROUND

A. Capital One Collected Customers' Sensitive PII, Promised To Keep It Safe, And Stored The PII In The AWS Cloud To The Benefit Of Both Capital One And AWS.

Capital One is one of the largest banks and credit card issuers in the United States, recording over $28 billion in revenue in 2019.[2] As a bank and credit card issuer, Capital One collects highly sensitive PII from applicants who apply for its credit cards, such as name, date of birth, address, phone number, self-reported income, Social Security number ("SSN"), and other identifying information. As part of this process, each applicant is provided with Capital One's Privacy Notice, which promises that—in exchange for providing their PII and applying for the credit card—Capital One will only use their PII for the enumerated purposes and will comply with

[2] Capital One 2019 Annual Report at 6, *available at* https://ir-capitalone.gcs-web.com/static-files/2f0f821a-0db0-4eab-9895-63013c4e59c2 (last visited April 28, 2021) (stating Capital One had $28.6 billion in revenue in 2019).

certain obligations to "protect" the PII "from unauthorized access and use." *See, e.g.*, Ex. 1.[3] Capital One has stipulated that the Privacy Notice contains one or more express contractual provisions regarding the safeguarding of Plaintiffs' PII with respect to the majority of the class. Doc. 1098.[4]

Because Capital One is a bank, the Privacy Notice issued by Capital One and provided to every applicant is, in fact, required under the Gramm-Leach-Bliley Act (the "GLBA"). To comply with its promises to applicants in its Privacy Notice that it will "use security measures that comply with federal law," Capital One must issue and follow Information Security Standards and Policies that it adopts as a company. *See* Ex. 3, Decl. of Brian Kelley ("Kelley") ¶¶ 38, 43, 45-46, 53-56. Capital One did issue such policies, but as described below, it failed miserably to follow them. *See* Ex. 4, Decl. of Stuart Madnick ("Madnick") at 33-34.[5]

Rather than comply with its contractual obligations to protect the treasure trove of sensitive data it had collected on approximately 98 million Americans, Capital One engaged in a perilous endeavor with AWS to become the *first* large financial institution to store its customers' data in the AWS cloud.[6] Defendants benefited financially from the move, but it came with substantial

[3] Exhibit numbers refer to the exhibits listed in the April 28, 2021, Declaration of Norman E. Siegel ("Siegel Decl.").

[4] Specifically, Capital One has admitted that the Privacy Notice contains enforceable contractual promises "with respect to safeguarding Plaintiffs' [PII]," at least as to those applicants who ultimately entered into cardholder agreements, which constitutes over [redacted]. *See* Doc. 1098, Stipulation; Ex. 2, Second Am. Supp. Resp. to Interrog. at Resp. to Interrog. 10 at 5. Plaintiffs intend to argue—as they did at the Motion to Dismiss stage—that the Privacy Notice contains enforceable contractual promises with respect to the entire class, including those applicants who did not ultimately enter into cardholder agreements. The term "customers" in this brief refers to applicants for Capital One's credit cards, regardless of whether their application ultimately resulted in a cardholder agreement.

[5] References to Professor Madnick's expert report are to its page numbers.

[6] *See, e.g.*, Ex. 5, Dep. Tr. Daniel Seeley at 21:24-22:2 ("[redacted]").

known security risks to the detriment of Plaintiffs and class members. These risks were compounded by the fact that Capital One retained and capitalized on class members' PII for years longer than it disclosed to customers. *See* Ex. 6, Decl. of Gary Olsen ("Olsen") ¶¶ 66-73; Ex. 7, Dep. Tr. Rule 30(b)(6) Kathy Kauffman at 74:15-77:10. AWS also profited from the endeavor in the form of huge contracts with Capital One, while paying little regard to the security of the sensitive data it knew Capital One was storing in the AWS cloud. Ex. 6, Olsen ¶¶ 63-65; Ex. 4, Madnick at 34-45.

B. Despite Repeated Opportunities, Defendants Failed To Remedy Known Vulnerabilities That Resulted In The Breach.

Despite Capital One's promises to its customers, and despite Capital One's and AWS's knowledge that Plaintiffs' PII was vulnerable to attack, Capital One and AWS did not keep Capital One's customers' highly sensitive PII safe.

To start, Capital One was aware *before* the Breach of three precise technical vulnerabilities exploited during the Breach, but failed to address any of them. *First*, Capital One's [redacted]—where class members' PII was stored in what are called S3 buckets (a component of the AWS cloud)—was guarded by a ModSecurity Web Application Firewall ("ModSec WAF"). Ex. 4, Madnick at 14-15, 17. [redacted], Capital One misconfigured the ModSec WAF [redacted]. *Id.* at 18. This misconfiguration, [redacted]. *Id.* It is undisputed that Capital One discovered [redacted]. *Id.* at 18-19. Therefore, in March 2019, at least one hacker

in the Breach, alleged to be former AWS employee Paige Thompson ("Thompson"), was able to exploit the ModSec WAF vulnerability, allowing her access to Plaintiffs' PII. *Id.* at 13-15.

Second, Capital One [redacted], that a well-known forgery vulnerability, known as a server-side request forgery ("SSRF"), could be used to access the AWS cloud Instance Metadata Service ("IMDS") to obtain valid Capital One Identity and Access Management ("IAM") credentials, also known as an IAM role. *Id.* at 19-20. Because Capital One took no action to remedy this vulnerability, or even monitor or alert for its exploitation, Thompson exploited the IMDS vulnerability and [redacted]. *Id.* at 20; *see also id*. at 14-15.

Third, Capital One was aware that the [redacted]. *Id.* at 20-22. If [redacted], Thompson would not have been able to view the data or download and exfiltrate it. *Id.* at 21-22. The risk of [redacted]—yet, again, no action was taken to remedy this vulnerability. *Id.*

Capital One has admitted that [redacted]. *See, e.g.*, Ex. 8, Capital One's Project Star Post-Incident Report at 2, 13; Ex. 9, Management's Root Cause Analysis at 1-2.[7] But discovery revealed that these technical vulnerabilities were symptoms of a much larger issue plaguing Capital One: its dysfunctional cyber organization, which suffered from pervasive, longstanding problems of which Capital One was well aware. For example, Capital One routinely failed to [redacted]

[7] Pagination for these two exhibits refers to the internal pagination of the reports.

[redacted]. Ex. 4, Madnick at 26-27. In 2018, a Capital One Enterprise Cyber Risk Report found that [redacted]. *Id.* at 19. This failure to timely address known vulnerabilities—including vulnerabilities that permitted the Breach—was the result of mismanagement by Capital One's senior management, [redacted]. *Id.* at 30. Capital One's former Managing Vice President of Cybersecurity Anthony Johnson described the dysfunction as "[redacted]," which impacted not only the organization's failure to address the high security risks but also resulted in high levels of attrition of employees with institutional knowledge of the problems. *Id.* at 32.

AWS, for its part, also knew *prior* to the Breach about the precise vulnerabilities exploited by Thompson, yet also took no action to remedy them. *First*, AWS [redacted]. *Id.* at 36-37. This vulnerability, which Thompson exploited in the Breach, [redacted] but was not remediated until November 2019—months after the Breach was discovered. *Id.* at 37-38. *Second*, AWS also was well aware that Capital One [redacted]. *Id.* at 40-41; *see also* Ex. 10, Dep. Ex. 208. Yet AWS failed to address Capital One's concerns, and an AWS employee admitted in his deposition that one of the main criteria in deciding whether to implement a customer's product feature requests was whether "[redacted]

[redacted]." Ex. 4, Madnick at 41. *Third*, AWS provided Capital One with a threat detection service called GuardDuty, which was supposed to alert Capital One to unauthorized access to the S3 buckets in the AWS cloud where Capital One was storing class members' PII. *Id.* at 43. But AWS's GuardDuty product had a [redacted]. *Id.* Steve Schuster, AWS's Director of Security Engineering and Operations, [redacted]." *Id.* (citing Schuster Dep. Tr. 92:17-23).

Finally, both Defendants were aware of a vulnerability that allowed Thompson to access class members' PII in the AWS cloud from *outside* of Capital One's environment: [redacted]. *Id.* at 44-45. Capital One employees [redacted], and AWS similarly [redacted]. *Id.* But neither Defendant took action until after the Breach, when both Defendants finally worked together to develop a "[redacted]." *Id.* at 45. If either Defendant had taken this action sooner, Thompson—[redacted]—would have been prevented from stealing class members' PII. *Id.* In all of the above-described instances, as well as many more developed throughout the course of discovery, both Defendants knew the risks and failed to act, resulting in the theft of class members' PII.

C. Despite Multiple Opportunities, Neither Defendant Timely Discovered The Breach.

Not only were Capital One and AWS fully aware of the precise vulnerabilities that led to the Breach, but the Breach also went undiscovered by Capital One and AWS despite the fact that the hacker downloaded a massive amount of data, accessed Capital One's environment at least five

times, and posted openly about her exploits online for several months. *Id.* at 13-14, 22-23, 28; Ex. 8, Project Star Report at 4-5. It was only after Capital One received an anonymous tip on July 17, 2019, about Thompson's public postings that Capital One finally recognized it had been hacked. Ex. 8 at 3, 5. Capital One and AWS should have discovered—and had multiple *opportunities* to discover—the Breach as early as March 2019. *See* Ex. 4, Madnick at 22-23, 28, 38-39.

Capital One has admitted that it had at least three opportunities to discover the Breach. *See id.* at 22-23, 28. The first opportunity occurred on March 22-23, 2019, the same days Thompson breached Capital One's environment and exfiltrated class members' PII. *Id.* at 13, 22. On those days, [redacted]; yet, as Capital One Cyber Security Operation Center's ("CSOC") post-Breach analysis found, [redacted]. *Id.* at 22-23. Capital One's second chance occurred on April 19, 2019, during which [redacted]. *Id.* at 23. Capital One also [redacted]. *Id.* at 23, 22 n.85. A final alert occurred on May 20, 2019, when AWS sent Capital One a handwritten note it had received which stated that Capital One had an "open socks proxy" at one of its IP addresses "that can hit IMS lots of security credentials." *Id.* at 28. Yet again, Capital One failed to identify that it had been breached, [redacted]. *Id.*; *see also* Ex. 8 at 4. These collective failures were the result of a deficient CSOC, which post-Breach, [redacted]. Ex. 4, Madnick at 22 n.83.

AWS also had at least two separate opportunities to discover the Breach prior to July 2019, the first being the May 20, 2019 note received by an AWS employee, which AWS sent to Capital One but failed to investigate thoroughly itself. AWS's second opportunity was through its use of "[redacted]. *Id.* 38-39. AWS uses [redacted]. *Id.* at 39. Despite [redacted]. *Id.*

D. Capital One Admitted Its Failures, And The Agencies That Regulate Capital One Determined [redacted].

In the wake of the Breach, Capital One has made multiple admissions with respect to its failures that resulted in the Breach. For example, in Capital One's post-Breach Management's Root Cause Analysis, [redacted]. *See* Ex. 9. Those [redacted]. *Id.* at

[8] To "tokenize" refers to the process of substituting a randomly generated identifier for a sensitive piece of data in order to prevent unauthorized access.

1-2. Capital One also [redacted]." *Id.* at 2-3.

The governmental agencies that regulate Capital One agreed that Capital One had failed in properly protecting the data entrusted to it. The Office of the Comptroller of the Currency ("OCC") and the Federal Reserve Board ("FRB") both issued findings and consent orders against Capital One, as well as a civil fine of $80 million. Exs. 11-12, OCC Consent Orders; Ex. 13, FRB Consent Order. In a [redacted]" Ex. 14, CAPITALONE_MDL_002213669, at -669-670 (italics and bolding in original). The OCC further found that [redacted]" *Id.* at -671.

E. The Impact Of The Breach For Approximately 98 Million Capital One Customers.

In the Breach, the attacker stole the PII of approximately 98 million Capital One customers. Ex. 2, at Resp. to Interrog. 10 at 5. Each and every customer is at risk of identity theft as a result of the Breach because the stolen PII can be used to commit identity theft. Ex. 15, Decl. of Kevin Mitnick ("Mitnick") ¶¶ 19-21, 61-71. Therefore, because each member of the class is at risk, each

member of the class will require identity theft and fraud monitoring to help prevent the harm to which Capital One and AWS have exposed them. *Id.* ¶¶ 61-71.

Capital One has advanced the narrative that the attacker did not distribute the breached data, but evidence in the record shows that she had the data on her computer and had clearly indicated in her statements that she planned to share or sell the data. Ex. 4, Madnick at 47, n. 259-260. Moreover, due to Capital One's [redacted]. *Id.* at 25-26, 34. The [redacted]. Ex. 27, Madnick Rebuttal Report at 9.[9] Critically, the evidence also shows that the Proposed Class Representatives have experienced identity theft and fraud in the wake of the Breach, many instances of which appear connected to the data stolen from Capital One, suggesting that the data was, indeed, further disseminated.[10]

[9] *See also* Ex. 28, M. Hedrick Dep. Tr. 59:8–60:7 ("[redacted]"). Further underlying the factual dispute as to whether there was another attacker, AWS's documents show that [redacted]. *See* Ex. 29, AWS Rule 30(b)(6) (Justin Christian) Dep. Tr. 85-88.

[10] Even if the data stolen by Thompson is not yet being shared or sold on the dark web, it is common for thieves to wait years before dumping or using data to commit fraud, and therefore Plaintiffs

Soon after the Breach, many of the Proposed Class Representatives[11] experienced fraud and identity theft. Exs. 16-22,[12] Plaintiffs' Resp. to Interrog. 4 and 6. Plaintiffs experienced unauthorized accounts opened or attempted to be opened in their names. Exs. 18, 19, 21, 22 at Resp. to Interrog. 4. The Plaintiffs who experienced identity theft in the form of opened or attempted unauthorized accounts suffered harm, including, for example, decreases in their credit scores, expending time filing police reports, freezing their credit, or spending money to mitigate the impact to their financial situations. Exs. 18, 21, 22 at Resp. to Interrog. 5. For example, Plaintiff Zielicke had an unauthorized account opened in his name that was used to spend tens of thousands of dollars and was subsequently registered as delinquent resulting in his credit score dropping several hundred points. Ex. 22, at Resp. to Interrog. 5. Plaintiff Gershen expended considerable time filing a police report after numerous credit cards, bank accounts, and loans were attempted to

---

remain at risk. Ex. 15, Mitnick ¶ 70. In any event, these are disputed factual questions not appropriate for determination at the class certification stage, and will be answered one way or the other as to the entire class.

[11] The Plaintiffs seeking appointment as Class Representatives are Emily Behar, Brandi Edmondson, Emily Gershen, Brandon Hausauer, Sara Sharp, John Spacek, Caralyn Tada, and Gary Zielicke. Doc. 971, ¶¶ 18-25.

[12] Capital One acknowledges that the Breach exposed the following information about Plaintiff Edmondson: [redacted]. Ex. 24, Revised and Verified Chart of Impacted Data for Proposed Class Representatives and Deposed MDL Plaintiffs (March 5, 2021). Thus, Plaintiff Edmondson is a member of the class with at least a contract claim and a claim for declaratory judgment and injunctive relief. Plaintiff Edmondson is representative of approximately [redacted] other members of the class whom Capital One has also admitted had data exfiltrated in the Breach, [redacted]. Ex. 2, pp. 5-7 ([redacted]). Furthermore, Capital One previously served a Verified Chart of Impacted Data claiming that Plaintiff Zielicke [redacted]). Ex. 25, Verified Updated Chart of Impacted Data (Nov. 10, 2020). Thus, of eight Proposed Class Representatives, Capital One under-reported exfiltrated data for three of them. Clearly it is possible that additional exfiltrated data for Plaintiff Edmondson will be discovered as well.

be opened in her name and she has been informed that the identity theft she experienced will impact the filing of her taxes this year and in the years to come. Ex. 18, at Resp. to Interrog. 5.

In addition to actual identity theft and fraud, Plaintiffs suffered harms in seeking to mitigate the effects of the Breach by purchasing identity theft and fraud monitoring services and devoting extra time to tracking their accounts and credit reports. Exs. 16-23, at Resp. to Interrog. 5. All Plaintiffs also face a substantial and ongoing risk of harm as a result of the Breach. Ex. 15, Mitnick ¶¶ 61-71. Further, Plaintiffs and class members lost the value of the unauthorized access to their PII, Ex. 6, Olsen ¶¶ 53-61, and the present value of prospective identity theft and fraud monitoring necessary to mitigate the continuing risk of harm. Ex. 15, Mitnick ¶¶ 69-71 and Ex. 26, Decl. of Terry M. Long ("Long") at 14; Ex. 30, Supp. Decl. of Terry Long ("Long Supplement") at 11. Finally, Capital One and AWS unjustly benefitted from their use of Plaintiffs' and class members' PII.

The harm to Plaintiffs is both imminent and ongoing. The vast amount of PII belonging to Plaintiffs and class members remains dangerously exposed and vulnerable to theft and fraud as currently maintained by both Defendants and used by Capital One. Capital One has not deleted the data or committed in its remediation efforts to deleting the data and neither Defendant has taken the required remediation steps to adequately protect the data. Ex. 4, Madnick at 46-50.

LEGAL STANDARD

A party moving for class certification must demonstrate that the proposed class meets the two-step inquiry outlined in Federal Rule of Civil Procedure 23. *See Gunnells v. Healthplan Servs., Inc.*, 348 F.3d 417, 423 (4th Cir. 2003). First, the movant must show that the proposed class meets the four prerequisites set forth in Rule 23(a):

> (1) *Numerosity*: "the class is so numerous that joinder of all members is impracticable";
> (2) *Commonality*: "there are questions of law or fact common to the class";

> (3) *Typicality*: "the claims or defenses of the representative parties are typical of the claims or defenses of the class"; and
> (4) *Adequacy*: "the representative parties will fairly and adequately protect the interests of the class."

Second, the district court must determine whether the proposed class meets one of the three requirements set forth in Rule 23(b). *Gunnells*, 348 F.3d at 423. For a damages class, Rule 23(b)(3) requires the court to find (1) that "questions of law or fact common to the members of the class predominate over any questions affecting only individual members" (the predominance requirement), and (2) that "a class action is superior to other available methods for the fair and efficient adjudication of the controversy" (the superiority requirement). Fed. R. Civ. P. 23(b)(3).

"A party seeking class certification must affirmatively demonstrate his compliance with . . . Rule [23]." *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011). Further, district courts have "an independent obligation to perform a 'rigorous analysis' to ensure that all of the prerequisites have been satisfied." *EQT Production Co. v. Adair*, 764 F.3d 347, 358 (4th Cir. 2014) (citing *Dukes*, 564 U.S. at 350-51). "In doing so, the district court may need to 'probe behind the pleadings before coming to rest on the certification question,' and to that end, may conduct, 'to the extent—but only to the extent—that they are relevant to determining whether the Rule 23 prerequisites for class certification are satisfied, an inquiry into the merits of the movant's claims and evidence.'" *In re Willis Towers Watson PLC Proxy Litig.*, 2020 WL 5361582, at *4 (E.D. Va. Sept. 4, 2020) (quoting *Amgen Inc. v. Conn. Ret. Plans & Trust Funds*, 568 U.S. 455, 466 (2013)) (internal citations omitted).

Still, district courts should "give Rule 23 a liberal rather than a restrictive construction, adopting a standard of flexibility in application which will in the particular case 'best serve the ends of justice for the affected parties and . . . promote judicial efficiency.'" *Gunnells*, 348 F.3d at 424. The question is not whether the plaintiffs will prevail on the merits, but rather, whether the

requirements of Rule 23 are met. *Id.* at 428 (citing *Eisen v. Carlisle & Jacquelin*, 417 U.S. 156, 177 (1974)). "[A] district court's 'wide discretion' in deciding whether to certify . . . a class" is based on its "greater familiarity and expertise than a court of appeals in managing the practical problems of a class action [thus] its certification decision is entitled to 'substantial deference,' especially when the court makes 'well-supported factual findings supporting its decision.'" *Ward v. Dixie Nat'l Life Ins. Co*., 595 F.3d 164, 179 (4th Cir. 2010) (internal citations omitted).

ARGUMENT

I. THE PROPOSED CLASSES

Plaintiffs seek certification pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(3), (b)(2), and if necessary, (c)(4), of the following classes:

- **The Applicant Class**: **All Applicants in the United States whose PII was compromised in the Breach.**[13] Plaintiffs Behar, Edmondson, Gershen, Hausauer, Sharp, Spacek, Tada, and Zielicke seek to represent this class in their claims of breach of contract, or in the alternative, breach of implied contract, against Capital One, and their claims of negligence, unjust enrichment, and declaratory judgment against Capital One and AWS.
- In the alternative, **The Cardholder Subclass**: **All Cardholders in the United States whose PII was compromised in the Breach.** A Cardholder is a current or former Capital One credit card holder.[14] Plaintiffs Behar, Edmondson, Gershen, Hausauer,

[13] The Applicant Class comprises the nationwide class pleaded in the representative complaint: "All persons in the United States whose PII was compromised in the Data Breach." Doc. 971, Second Am. Compl. ("Compl.") ¶ 144.

[14] Although all members of the alternatively proposed Cardholder Subclass are members of the Applicant Class, Capital One has taken conflicting positions with respect to whether applicants who never became cardholders have contract claims through the Privacy Notice. Therefore, Plaintiffs propose the Cardholder Subclass, which consists of applicants who have cardholder

Sharp, Spacek, Tada, and Zielicke[15] seek to represent this subclass in their claims of breach of contract, or in the alternative, breach of implied contract, against Capital One, and their claims of negligence, unjust enrichment, and declaratory judgment against Capital One and AWS.

- In the alternative to certification of the Applicant Class and/or the Cardholder Subclass, **The SSN / Bank Account Subclass**: **All persons in the United States whose Social Security number or bank account and routing number was compromised in the Breach.** Plaintiffs Hausauer and Behar seek to represent this subclass in their claims of breach of contract, or in the alternative, breach of implied contract, against Capital One, and their claims of negligence, unjust enrichment, and declaratory judgment against Capital One and AWS.
- **The California Subclass**: **All persons in California whose PII was compromised in the Breach.** Plaintiffs Hausauer and Tada seek to represent this subclass in their claims of violation of the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*, against Capital One and AWS.
- **The California CLRA Subclass**: **All persons in California who sought or acquired a Capital One credit card for personal, family, or household purposes, and whose PII was compromised in the Breach.** Plaintiff Tada seeks to represent this subclass

agreements, in anticipation of arguments by Capital One regarding this as-yet unsupported position in the case.

[15] These Plaintiffs pursue claims that are unified across both the Applicant Class and the alternatively proposed Cardholder Subclass and are typical of and adequate to represent victims of the Breach nationwide. In the event the Court requires a class representative who is only an Applicant—and not a Cardholder—such a plaintiff can readily be added by substitution or amendment.

in their claims of violation of the California Consumer Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, *et seq.*, against Capital One.

- **The Florida Subclass**: **All persons in Florida whose PII was compromised in the Breach.** Plaintiffs Behar and Zielicke seek to represent this subclass in their claims of violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201, *et seq.*, against AWS.
- **The New York Subclass**: **All persons in New York whose PII was compromised in the Breach.** Plaintiff Gershen seeks to represent this subclass in their claims of violation of the New York General Business Law ("GBL"), N.Y. Gen. Bus. Law §§ 349, *et seq.*, against Capital One and AWS.
- **The Washington Subclass**: **All persons in Washington whose PII was compromised in the Breach.** Plaintiff Sharp seeks to represent this subclass in their claims of violation of the Washington Consumer Protection Act ("WCPA"), Wash. Rev. Code Ann. §§ 19.86.02, *et seq.*, against Capital One and AWS.

Excluded from each proposed class are Defendants, any entity in which any Defendant has a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from each proposed class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

The classes meet the requirements for certification with respect to the alleged claims, as set forth below.

II. ARTICLE III STANDING

In order to have Article III standing, the Plaintiffs must demonstrate: "(1) they suffered an injury-in-fact that was concrete and particularized and either actual or imminent; (2) there was a

causal connection between the injury and the defendant's conduct (i.e. traceability); and (3) the injury was likely to be redressable by a favorable judicial decision." *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 618-19 (4th Cir. 2018). Where, as here, the Defendants experienced a Breach in which a hacker exfiltrated Plaintiffs' PII and that of 98 million other Americans, and many Plaintiffs have subsequently experienced identity theft using their PII, standing is satisfied. *See, e.g.*, *id.* at 619, 623 (allegations of misuse of personal data made it both "plausible and likely" that their injury was due to a data breach of the defendant's data systems, even where the defendant in that case denied that a data breach had even occurred). Just as in *Hutton*, shortly after the Breach here, several Plaintiffs "began to notice that fraudulent [] accounts were being opened in their names. . . ." *Id.* at 623.[16] This is no surprise given the type of information exfiltrated in the Breach. As Plaintiffs' expert explains:

[redacted]

Ex. 15, Mitnick ¶¶ 62-63.

Importantly, Plaintiffs have already demonstrated their standing in their response to Defendants' motions to dismiss. *See* Doc. 427 at 9-16. Indeed, this Court has held that Plaintiffs having "suffered actual misuse of their PII" raises "the plausible inference that Thompson shared

[16] For example, on or about July 31, 2019, Plaintiff Gershen learned that [redacted]. Ex. 18, at Resp. to Interrog. 4. Plaintiff Zielicke had an [redacted]. Ex 22, at Resp. to Interrog. 4. Plaintiff Sharp had an [redacted]. Ex. 19, at Resp. to Interrog. 4. Plaintiff Tada had a [redacted]. Ex. 21, at Resp. to Interrog. 4.

the information with others or enabled others to receive that information and plausibly connecting the Data Breach to Plaintiffs' alleged injuries." Doc. 879 at 28. This Court further held: "Based on these allegations, it is also plausibly alleged that there exists, beyond the speculative level, the imminent threat of identity theft." *Id.* (citing *In re Marriott Int'l, Inc.*, 440 F. Supp. 3d 447, 462-65 (D. Md. 2020)). Additionally, the claims of unjust enrichment, and entitlement to nominal damages upon proof of a contract or implied contract and its breach, satisfy the requirements of Article III standing.[17] Thus, Proposed Class Representatives have standing to pursue this class action.

III. PLAINTIFFS SATISFY THE REQUIREMENTS OF RULE 23(a).

A. Joinder Of All Proposed Class Members Is Impracticable.

"Generally, class sizes of forty or more are considered sufficiently numerous to satisfy Rule 23(a)'s numerosity requirement. . . ." *In re Zetia (Ezetimibe) Antitrust Litig.*, 481 F. Supp. 3d 571, 574 (E.D. Va. 2020). Capital One concedes that [redacted] customers who applied for credit in the United States had their data exfiltrated in the Breach, of whom approximately [redacted] became cardholders. Ex. 2, Resp. to Interrog. 10 at 5. The SSN / Bank Account Subclass comprises approximately [redacted] individuals. *Id.* at 7-8. As for the State Subclasses, approximately

[17] *Cf. Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 802 (Mar. 8, 2021) (holding that a nominal damages claim satisfies redressability prong; stating "every violation [of a right] imports damages") (internal citation omitted); *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1623 (2020) (Thomas, J., concurring) (similar); *Frank v. Gaos*, 139 S. Ct. 1041, 1047 (2019) (Thomas, J., dissenting) ("[A] plaintiff seeking to vindicate a private right need only allege an invasion of that right to establish standing."); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1551 (2016), *as revised* (May 24, 2016) (Thomas, J., concurring)) ("In a suit for the violation of a private right," including contract rights and unjust enrichment, "courts historically presumed that the plaintiff suffered a *de facto* injury merely from having his personal, legal rights invaded."); *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 154 (4th Cir. 2000) ("One can readily recognize that . . . a party to a breached contract bears the kind of claim that he may press in court.").

[redacted] Breach victims were California residents; [redacted] Florida; [redacted] New York; and [redacted] Washington. *Id.* at 5-7. The proposed classes are sufficiently numerous.

B. Defendants' Conduct Related To The Breach Raises Common Legal And Factual Questions.

"Rule 23(a)(2) requires the existence of 'questions of law or fact common to the class.'" *Bryant v. King's Creek Plantation, L.L.C.*, 2020 WL 6876292, at *4 (E.D. Va. June 22, 2020). "[A]t least one question needs to be 'capable of class-wide resolution—which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke.'" *Id.* (quoting *Dukes*, 564 U.S. at 350). A single common question is sufficient. *See Ealy v. Pinkerton Gov't Servs., Inc.*, 514 F. App'x 299, 307 (4th Cir. 2013). The claims here easily meet this standard.

Each class member's PII was compromised in the Breach due to the Defendants' failures to remedy multiple known technical vulnerabilities in the security of information collected and maintained by Capital One and stored on the AWS cloud. *See* Factual Background § B (discussing (1) ModSec WAF, (2) SSRF, and (3) overpermissioned roles vulnerabilities). Therefore, proof of what Defendants knew and what they did or did not do to address these vulnerabilities is common to all class members. Furthermore, proof that the attacker exploited these vulnerabilities to exfiltrate their PII is common to all class members. The requisite commonality exists here because the issues raised by the class's claims have common answers that will drive the litigation. *See Brown v. Nucor*, 785 F.3d 895, 909 (4th Cir. 2015) (citing *Dukes*, 564 U.S. at 350). These include, for example:

- Whether Capital One breached promises made in its Privacy Notice by failing to protect class members' PII from "unauthorized access and use" and by failing to "use security measures that comply with federal law" including "computer safeguards and secured files and buildings";

- Whether Capital One's breached promises resulted in the attacker exfiltrating class members' PII in the Breach;
- Whether and to what extent Capital One's breached promises caused harm to Plaintiffs and class members;
- Whether Defendants owed a duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and class members' PII;
- Whether Defendants breached that duty;
- Whether and when Defendants knew about the security risks posed by their technical vulnerabilities;
- Whether Defendants' failure to remedy obvious and known security risks posed by their technical vulnerabilities was negligent;
- Whether Defendants' negligence caused the Plaintiffs' and class members' harm;
- Whether Defendants were unjustly enriched;
- Whether Capital One's inadequate data security violated California's UCL, New York's GBL, and/or Washington's CPA;
- Whether AWS's inadequate data security violated California's UCL, Florida's DUTPA, New York's GBL, and/or Washington's CPA;
- Whether Capital One's misrepresentations or omissions regarding the inadequacy of its data security violated California's UCL and CLRA, New York's GBL, and/or Washington's CPA;
- Whether AWS's failure to disclose it did not maintain sufficient data security for the protection of class members' PII violated California's UCL, Florida's DUTPA, New York's GBL, and/or Washington's CPA;
- Whether Defendants' violations of these state statutes harmed Plaintiffs and class members; and
- Whether Defendants' security is still inadequate to protect Plaintiffs' and class members' PII, such that injunctive relief is warranted.

C. Plaintiffs' Claims Are Typical Of Those Of The Class.

Under Rule 23(a)(3), typicality is demonstrated when "the representative party's interest in prosecuting his own case [] simultaneously tend[s] to advance the interests of the absent class members." *Dieter v. Microsoft Corp.*, 436 F.3d 461, 466 (4th Cir. 2006). Typicality does not

require "that the plaintiff's claim and the claims of the class members be perfectly identical or perfectly aligned." *Id.* at 467. However, where "the facts on which the plaintiff would necessarily rely to prove [his *prima facie* case] . . . would also prove the claims of the absent class members," typicality is satisfied. *Id.* Here, Plaintiffs' claims and legal theories arise under the same factual predicate as those of the class members. Their PII was compromised in the same Breach, which was caused by the same vulnerabilities the Defendants created and permitted to persist. Once Plaintiffs prove their contract, implied contract, unjust enrichment, negligence, and applicable state statutory claims, based on this factual predicate, they will prove the same claims on behalf of other class members. The elements Plaintiffs must prove are identical to what absent class members would have to prove, and no defenses are unique to Plaintiffs. Thus, typicality is satisfied.

D. Plaintiffs And Proposed Class Counsel Will Fairly And Adequately Protect The Interests Of The Proposed Classes.

Rule 23(a)(4) requires the class representative to show that they "will fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). "[B]asic due process requires that named plaintiffs possess undivided loyalties to absent class members." *Broussard v. Meineke Disc. Muffler Shops, Inc.*, 155 F.3d 331, 338 (4th Cir. 1998). "Distilled to its essence, the adequacy inquiry focuses on two questions:

(i) Has plaintiff demonstrated the requisite level of knowledge and control of the litigation to ensure that he will vigorously prosecute the claims asserted here and
(ii) Has plaintiff demonstrated the requisite credibility to ensure he will act as a fiduciary with respect to the class he seeks to represent.

Shiring v. Tier Technologies, Inc., 244 F.R.D. 307, 315 (E.D. Va. 2007). Plaintiffs have vigorously prosecuted the claims in this case. While some Proposed Class Representatives possess claims under particular state statutes or under particular factual circumstances, i.e., whether they ultimately became cardholders, all claims are similar in their essence and arise from the same set

of facts focused on Defendants' uniform conduct vis-à-vis a single occurrence—the Breach. No conflict or appearance of any conflict exists. These Plaintiffs have participated actively in this case by reviewing pleadings, responding to discovery, and sitting for lengthy depositions, all of which demonstrate their "requisite level of knowledge and control of the litigation." *Id.*; Exs. 16-23; Siegel Decl. ¶¶ 17-24, 34-35.

Under Rule 23(a)(4), a court must also find that class counsel is "qualified, experienced and generally able to conduct the proposed litigation." *McLaurin v. Prestage Foods, Inc.*, 271 F.R.D. 465, 476 (E.D.N.C. 2010) (citation omitted). Proposed Class Counsel, selected by this Court as interim lead counsel, are experienced class action attorneys who have demonstrated their commitment to prosecuting this case. *See* Docs. 135, 136, 140, and 210; Siegel Decl. ¶¶ 36-41. Steven T. Webster, designated by this Court as local counsel for Plaintiffs in this litigation, is an experienced attorney in the Eastern District of Virginia, and has demonstrated his commitment to serving as Liaison Counsel in this case. Doc. 249; Siegel Decl. ¶ 37. Among other tasks, class counsel have to date: (1) propounded and responded to discovery and engaged in many months of discovery motion practice; (2) successfully defended against Defendants' Motions to Dismiss; (3) reviewed over 374,000 documents; (4) deposed 22 current and former Capital One employees and 8 current and former AWS employees; (5) deposed 14 corporate representatives under Rule 30(b)(6); (6) defended eight depositions of the Proposed Class Representatives and nine MDL Plaintiff depositions; (7) engaged experts and served five expert reports relating to Defendants' negligent security practices, appropriate equitable relief to change those practices and models for class members' recovery, and Plaintiffs' damages and risk of harm, and offered those experts for depositions (which are ongoing); and (8) funded the entirety of the litigation. Siegel Decl. ¶¶ 38-41. Thus, Plaintiffs and proposed Rule 23(g) class counsel meet the adequacy requirement.

E. Class Membership Is Readily Ascertainable.

The Fourth Circuit has "repeatedly recognized that Rule 23 contains an implicit threshold requirement that the members of a proposed class be readily identifiable." *Soutter v. Equifax Info. Servs., LLC*, 307 F.R.D. 183, 196 (E.D. Va. 2015) (quoting *EQT Prod. Co.*, 764 F.3d at 358) (internal quotations omitted). This is also known as the "ascertainability" requirement. Plaintiffs need only "demonstrate that class members will be identifiable without extensive and individualized fact-finding or mini-trials." *Id.* Class membership here is identified through Capital One's detailed records of all individuals whose PII was exfiltrated in the Breach. Such clear and objective indicia of membership in the classes proposed here are "sufficiently definite so that it is administratively feasible for the court to determine whether a particular individual is a member," meeting the Fourth Circuit's implied ascertainability requirement. *Manuel v. Wells Fargo Bank, N.A.*, 2015 WL 4994549, at *6 (E.D. Va. Aug. 19, 2015) (internal citations omitted).

IV. PLAINTIFFS SATISFY THE REQUIREMENTS OF RULE 23(b)(3).

Rule 23(b)(3) requires "that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). The record and applicable precedents show that predominance and superiority are satisfied here.

A. Predominance Is Satisfied.

"The 'predominance inquiry tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation.'" *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016) (quoting *Amchem Products, Inc. v. Windsor*, 521 U.S. 591, 623 (1997)). In assessing predominance, a district court considers the "relation between common and individual questions in a case." *Id.* "An individual question is one where 'members of a proposed class will need to

present evidence that varies from member to member,' while a common question is one where 'the same evidence will suffice for each member to make a prima facie showing [or] the issue is susceptible to generalized, class-wide proof.'" *Id.* (quoting 2 W. Rubenstein, Newberg on Class Actions § 4:50, pp. 196–197 (5th ed. 2012)) (alteration in original). "The predominance inquiry 'asks whether the common, aggregation-enabling, issues in the case are more prevalent or important than the non-common, aggregation-defeating, individual issues.'" *Id.* (quoting Newberg, § 4:49, at 195-196).

"If 'common questions represent a significant aspect of a case and . . . can be resolved for all members of a class in a single adjudication,' then they predominate over individual questions." *Bryant*, 2020 WL 6876292, at *4 (quoting *Messner v. Northshore Univ. HealthSystem*, 669 F.3d 802, 815 (7th Cir. 2012)) (alteration in original). "Each plaintiff's claim 'need not be identical' to satisfy the predominance requirement." *Id.* (quoting *Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 658 (4th Cir. 2019), *cert. denied*, 140 S. Ct. 676 (2019)). "When 'one or more of the central issues in the action are common to the class and can be said to predominate, the action may be considered proper under Rule 23(b)(3) even though other important matters will have to be tried separately, such as damages or some affirmative defenses peculiar to some individual class members.'" *Tyson Foods*, 577 U.S. at 453 (quoting 7AA C. Wright, A. Miller, & M. Kane, Federal Practice and Procedure § 1778, pp. 123–124 (3d ed. 2005)).

1. Common questions predominate Plaintiffs' express contract claim against Capital One, and their alternative implied contract claim.

All parties agree that Virginia's substantive law applies to the common law claims of all class members. *See* Docs. 1092, 1103, 1105, 1106. Under Virginia law, the elements of a claim for breach of contract are: "(1) a legally enforceable obligation of a defendant to a plaintiff; (2) the defendant's violation or breach of that obligation; and (3) injury or damage to the plaintiff caused

by the breach of obligation." *Filak v. George*, 594 S.E.2d 610, 619 (Va. 2004). Plaintiffs allege Capital One breached its standard form Privacy Notice, where Capital One promised that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings." *See* Ex. 3, Kelley ¶ 38; Ex. 1, Privacy Notice. The Privacy Notice also lists the circumstances in which Capital One is permitted to disclose its customers' PII to third parties, which does not include the circumstances in which it was disclosed here. *See id.*

Plaintiffs contend Capital One is bound by the Privacy Notice as to all class members—applicants, current customers, and former customers alike. *See* Compl. ¶ 96. Capital One admits there was a Privacy Notice in effect throughout the class period.[18] *See* Doc. 1139 at 5 n.4. Moreover, the Court has already concluded that class members and Capital One assented to the

[18] Capital One's Privacy Notice in effect from 2005 to 2009 contains immaterial differences in Capital One's data security obligations from that in effect from 2010 to 2019. All versions of the Privacy Notice require Capital One to maintain electronic safeguards and secure buildings to protect class members' PII. *See* Ex. 3, Kelley ¶¶ 34-35 (detailing Capital One's Privacy Notices from 2005 to 2009, which state: "We maintain physical safeguards, such as secure areas in buildings; electronic safeguards, such as passwords and encryption; and procedural safeguards, such as customer authentication procedures to protect against ID theft."); *id.* ¶ 38 (detailing Capital One's Privacy Notices from 2010 to 2019, stating "[W]e use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."); *see also* Ex. 31 (copy of example Privacy Notice pre-2010); Ex. 32 (copy of example Privacy Notice post-2010). While the 2010 to 2019 Privacy Notices state that Capital One will employ security measures that "comply with federal law" and the 2005 to 2009 Privacy Notices do not contain this statement, this additional descriptive statement is not a material additional obligation from those contained in the 2005 to 2009 versions. Ex. 3, Kelley ¶ 55. Rather, Capital One merely says that the security measures it will employ comply with federal law, and those security measures are materially identical to the measures Capital One promises to employ in its 2005 to 2009 Privacy Notices. Both versions "promise the bank's customers and consumers that it has implemented information security policies, procedures, and programs that are required by and in compliance with the GLBA and other federal and state regulation." *Id.* In other words, both versions reference Capital One's written Information Security Policy and Standards. *Id.* ¶ 52. Moreover, the relevant federal law in effect (namely, Section 5 of the FTC Act, 15 U.S.C. § 45, and GLBA, 15 U.S.C. §§ 6801.1 *et seq.*, and relevant supporting regulations), was the same throughout the class period. *See, e.g.*, *id.* ¶¶ 20, 35-38, 46.

terms of the Privacy Notice. *See* Doc. 879 at 41-42 ("[T]here is an objective manifestation of assent by both parties to enter into a contractual relationship based on specific referenced terms, which included the privacy notices (and data security promises therein)."). Capital One contends, however, that the Privacy Notice is only enforceable through the Cardholder Agreement, and thus, only by cardholders, and not by applicants who were denied credit and never became cardholders. Capital One has never explained this dichotomy; however, the question whether the Privacy Notice is a stand-alone agreement or, conversely, is only enforceable by way of incorporation through the Cardholder Agreement, is a common legal question that will be answered the same way, one way or the other, for every class member. Further, Capital One's records identify who applied for credit and when, and whether that application was approved or declined.[19] Therefore, class members who applied for credit and were declined, and thus, who are impacted by the legal ruling of whether the Privacy Notice is enforceable absent a Cardholder Agreement, are identifiable and ascertainable.[20]

[19] Ex. 2, Capital One's Resp. to Interrog. 10 at p. 5 (identifying that of the [redacted] individuals impacted in the Breach, "[redacted]").

[20] Such individuals are entitled to bring a claim for breach of implied contract and for unjust enrichment in the alternative to their breach of express contract claim under the Court's ruling denying Capital One's motion to dismiss these claims. Doc. 879 at 44, 47. Thus, to the extent the Court concludes non-cardholder class members are *not* entitled to enforce the Privacy Notice, these identifiable class members would be entitled to proceed on these quasi-contract theories. Because a claim for breach of implied-in-fact contract contains the same elements as a claim for breach of express contract, only differing in that an implied-in-fact contract is not reduced to writing or oral agreement and is instead inferred "from the course of conduct of the parties," *see McConnell v. Servinsky Eng'g, PLLC*, 22 F. Supp. 3d 610, 618 (W.D. Va. 2014), this claim also satisfies predominance. Plaintiffs allege Capital One's act of taking possession of PII created the implied contractual obligation to protect it, and that Capital One breached this obligation by failing to provide adequate security measures and by disclosing that information to unauthorized third parties. *See* Doc. 879 at 46. Because Capital One took possession of every class member's PII, its implied contractual obligations arose for each of them (for whom there is no enforceable Privacy Notice), and its failure to use adequate security measures is also common to every class member. Further, as explained in Part IV.A.2, below, common issues also predominate with respect to Plaintiffs' unjust enrichment claim.

Thus, the next issue is whether the question of Capital One's liability for breach of the Privacy Notice has a common answer for every class member to whom it applies. The answer is yes, because the Privacy Notice is a standardized, non-negotiated adhesion contract, and Capital One's deficient performance under it is common to all class members. Courts routinely conclude that cases involving an alleged breach of a form contract meet the requirements for class certification because each contract will be interpreted the same way, one way or the other, for each class member. *See In re TD Bank, N.A. Debit Card Overdraft Fee Litig.*, 325 F.R.D. 136, 157 (D.S.C. 2018) (certifying class as to the claim defendant bank breached "contracts of adhesion, involving non-negotiable terms and a vast bargaining/information imbalance between the parties," stating the "common sense principle" that "standardized agreements should be 'interpreted wherever reasonable as treating alike all those similarly situated, without regard to their knowledge or understanding of the standard terms of the writing.'") (quoting Restatement (Second) of Contracts § 211(2)); *In re Med. Cap. Sec. Litig.*, 2011 WL 5067208, at *3 (C.D. Cal. July 26, 2011) ("Courts routinely certify class actions involving breaches of form contracts.") (citing *Sacred Heart Health Systems, Inc. v. Humana Military Healthcare*, 601 F.3d 1159, 1171 (11th Cir. 2010) ("It is the form contract, executed under like conditions by all class members, that best facilitates class treatment"); *Smilow v. Southwestern Bell Mobile Systems, Inc.*, 323 F.3d 32, 42 (1st Cir. 2003) ("Overall, we find that common issues of law and fact predominate here. The case turns on interpretation of the form contract, executed by all class members and defendant.")).[21]

[21] *See also Allapattah Servs. v. Exxon Corp.*, 333 F.3d 1248, 1261 (11th Cir. 2003); *Dupler v. Costco Wholesale Corp.*, 249 F.R.D. 29, 37-38 (E.D.N.Y. 2008) (collecting cases for the proposition that class certification is typically appropriate in cases involving form contracts); *Winkler v. DTE, Inc.*, 205 F.R.D. 235, 243 (D. Ariz. 2001) (rejecting argument that individual issues would predominate in breach of contract claim where standard form contracts were used); *Mortimore v. F.D.I.C.*, 197 F.R.D. 432, 438 (W.D. Wash. 2000) ("Since this case involves the use of form contracts, it is particularly appropriate to use the class action procedure."); *Haroco, Inc. v.*

Therefore, the first two elements for breach of contract—a legally enforceable obligation and Capital One's breach—have a common answer for all class members making Capital One's liability for breach of contract appropriate for class certification. In addition, the question of class members' remedies attributable to Capital One's breach of contract or implied contract can also be resolved on a class basis.

Crucially, nominal damages are available—in fact, required—when a contract is broken. Under Virginia law—which applies to all claims here—nominal damages are presumed upon proof of breach. *Paulette v. Paulette*, 2000 WL 196788, at *2 (Va. Ct. App. Feb. 22, 2000) ("upon the breach of a valid and binding contract the law infers nominal damages"); *see also W. Insulation, LP v. Moore*, 316 F. App'x 291, 298-99 (4th Cir. 2009) (construing Virginia law). The entitlement to nominal damages is sufficiently automatic that Virginia law deems a breach of contract claim to fully accrue, for limitations purposes, at the time of breach (because, at a minimum, the remedy of nominal damages becomes enforceable at the time of breach). *See, e.g.*, *Kerns v. Wells Fargo Bank, N.A*, 818 S.E.2d 779, 785-86 (Va. 2018). Courts have often certified claims seeking nominal damages. For example, in *Opperman v. Path, Inc.*, 2016 WL 3844326, at *15-16 (N.D. Cal. July 15, 2016), the court certified a Rule 23(b)(3) class seeking nominal damages for a privacy tort claim precisely because "the problems of proof which attend Plaintiffs' claims for compensatory damages are absent in regard to their claim for nominal damages," where the amount of damages is necessarily uncertain. *Id.* at *16; *see also Davis v. Abercrombie*, 2014 WL 4956454, at *25 (D.

American Nat. Bank and Trust Co. of Chicago, 121 F.R.D. 664, 669 (N.D. Ill. 1988) ("Since plaintiffs' claims arise from allegations of common practice and rights derived from form contracts, the case appears to present the classic case for treatment as a class action.") (internal quotations omitted); *Kleiner v. First Nat'l Bank of Atlanta*, 97 F.R.D. 683, 692 (N.D. Ga. 1983) (noting that "claims arising from interpretations of a form contract appear to present the classic case for treatment as a class action, and breach of contract cases are routinely certified as such," and citing numerous cases in which such claims were certified).

Haw. Sept. 30, 2014) (certifying damages class; stating "Plaintiffs and each class member will be entitled to an award of nominal damages") (citing *Cummings v. Connell*, 402 F.3d 936 (9th Cir. 2005)).

In addition to nominal damages, Plaintiffs' other damages methodologies use "readily-applied, mechanical computation" of class-wide data produced by Capital One, such that common issues continue to predominate over individual ones. *See* 1 McLaughlin on Class Actions ("McLaughlin") § 5:23 (17th ed.). Mr. Olsen identifies the value of the hacker's unauthorized access to the PII through a market valuation of the various data elements exfiltrated in the Breach, a calculation that can be applied mechanistically to the class as a whole or to any individual Plaintiff or class member. Ex. 6, Olsen ¶¶ 55-61. And Mr. Long calculates the cost of access to ongoing identity theft and fraud monitoring services necessitated by Capital One's breach of contract through its lax data security, using Capital One's data as to the number and birth dates of class members and standard actuarial techniques. Ex. 26, Long at 4-13; Ex. 30, Long Supplement at 3-10.[22] These models measure damages to each class member resulting from Capital One's failure to adequately protect class members' PII in breach of its contracts or implied contracts, thus satisfying *Comcast Corp. v. Behrend*, 569 U.S. 27 (2013). *See* McLaughlin, § 5.23 & n.74. Common questions predominate as to Plaintiffs' contract claims.

2. Common questions predominate Plaintiffs' claims for unjust enrichment against Capital One and AWS.

"Broadly stated, the elements of an unjust enrichment claim are the receipt of a benefit and the unjust retention of the benefit at the expense of another." Doc. 879 at 43 (citing, *inter alia*, *Schmidt v. Household Finance Corp.*, 661 S.E.2d 834 (Va. 2008); Restatement (First) of

[22] Plaintiffs also seek disgorgement of Capital One's profits arising from the use of the PII for credit risk and fraud monitoring. *See* Ex. 6, Olsen ¶¶ 66-73; Restatement (Third) of Restitution and Unjust Enrichment § 39 (2011) (disgorgement remedy for breach of contract).

Restitution § 1 cmt. b (1937) ("A person confers a benefit upon another if he gives to the other possession of or some other interest in money, land, chattels, or choses in action, performs services beneficial to or at the request of the other, satisfies a debt or a duty of the other, or in any way adds to the other's security or advantage."); *see also Adair v. EQT Prod. Co.*, 320 F.R.D. 379, 403 (W.D. Va. 2017) ("The elements of a claim for unjust enrichment are (1) the plaintiff conferred a benefit on the defendant; (2) the defendant knew of the benefit and should reasonably have expected to repay the plaintiff; and (3) the defendant accepted or retained the benefit without paying for its value.") (internal quotations omitted). "[R]esolution of the unjust enrichment claim will turn on the substantive equity or inequity of the practice" at issue. *In re TD Bank*, 325 F.R.D. at 160.

Courts routinely conclude a claim of unjust enrichment can be resolved class-wide when the alleged inequitable conduct relates to common corporate policies and practices. *See id.* at 160-61 (citing *In re Checking Account Overdraft Litig.*, 286 F.R.D. 645, 657 (S.D. Fla. 2012) ("Unjust enrichment claims can be certified for class treatment where there are common circumstances bearing on whether the defendant's retention of a benefit received from class members was just or not."); *In re Checking Account Overdraft Litig.*, 275 F.R.D. 666, 680 (S.D. Fla. 2011) (certifying unjust enrichment class because the focus was on the defendant bank's uniform conduct and disclosures).

Here, each member of the proposed class conferred their PII on Defendants, which Defendants used for business and to earn profits. *See* Ex. 6, Olsen ¶¶ 22-27, 66-73. Because Capital One aggregated and mined this PII *en masse* and used it collectively for various product development and marketing purposes to increase profitability, and because AWS used Capital One's retention of the PII to generate profits from Capital One's use of its cloud computing

product, whether each class member's conferral of their PII benefitted each Defendant is a question that will be answered the same way for each class member. Likewise, the elements of Defendants' knowledge of the benefit and whether they should have expected to pay for the value conferred, and whether Defendants accepted or retained the benefit without paying for its value, each focus on Defendants' conduct, not any class member's, and therefore, these elements will also be resolved the same way for each class member.[23] *See* Doc. 879 at 44 ("[C]ourts have concluded that the failure to secure a party's data can give rise to an unjust enrichment claim where a defendant accepts the benefits accompanying plaintiff's data and does so at the plaintiff's expense by not implementing adequate safeguards, thereby making it 'inequitable and unconscionable' to permit defendant to retain the benefit of the data (and any benefits received therefrom), while leaving the plaintiff party to live with the consequences.") (citing *Sackin v. Transperfect Global, Inc.*, 278 F. Supp. 3d 739, 751 (S.D.N.Y. 2017); *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014)). Accordingly, predominance is satisfied as to Plaintiffs' unjust enrichment claim.

3. Common questions predominate Plaintiffs' negligence claims against Capital One and AWS.

"The elements of an action in negligence are a legal duty on the part of the defendant, breach of that duty, and a showing that such breach was the proximate cause of injury, resulting in

[23] Plaintiffs' expert estimates the unjust enrichment to AWS through its profits generated by the Capital One relationship, and to Capital One through its profits generated using PII for account takeover fraud and transaction fraud monitoring and prevention. Ex. 6, Olsen ¶¶ 66-73. Plaintiffs also seek from Defendants the market value of access to the PII under Restatement (Third) of Restitution and Unjust Enrichment §§ 49-51 (restitution of market value of benefit). Estimating the amount to be disgorged does not focus on individual issues among class members; thus, Mr. Olsen's estimates do not raise any concern that individual issues predominate or pose any other barrier to Rule 23(b)(3) class certification.

damage to the plaintiff." *Blue Ridge Serv. Corp.of Virginia v. Saxon Shoes, Inc.*, 624 S.E.2d 55, 62 (Va. 2006). This Court has already recognized a duty to protect PII independent of any duty arising under contract, Doc. 879 at 18-24, and the necessary factual proof related to that tort duty will focus on the conduct of Capital One and AWS, and not individualized facts relating to class members. The same is true of the breach element. Plaintiffs will present common evidence of Defendants' conduct to prove that "Capital One and Amazon, aware of the vulnerabilities and risks associated with their servers on which they stored Plaintiffs' PII, failed to take reasonable care to protect Plaintiffs' PII from unauthorized access, increasing the risk of harm." Doc. 879 at 24; *see* Factual Background § B-D; *see generally* Ex. 4, Madnick. Because all class members transferred their PII to Capital One (and thus to AWS) and all suffered theft of their PII, whether Defendants employed inadequate data security, and whether that inadequate security was a cause of the Breach, is a common, predominating question that will be answered the same way for each class member.

Common evidence also supports causation. First, whether Defendants' inadequate security caused the Breach is a common question with a common answer. Through expert testimony, Plaintiffs can show that all class members face increased risk of identity theft and other fraud because of the exfiltrated PII. *See* Ex. 15, Mitnick ¶¶ 19-21, 62-63. While Defendants will undoubtedly contend that the stolen PII was fully recovered by the FBI—a contention that is hotly contested based on the discovery—that causation-related question applies to and has a common answer for all class members, reinforcing the propriety of Rule 23(b)(3) certification. Finally, while Defendants may challenge proximate cause by asserting, for example, that other data breaches break any causal link between the criminal exfiltration from Capital One and the subsequent injuries to Plaintiffs and the class, the concurrent cause doctrine prevents such a harsh result. *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 988 (N.D. Cal. 2016)

("[U]nder Defendants' theory, a company affected by a data breach could simply contest causation by pointing to the fact that data breaches occur all the time, against various private and public entities. This would, in turn, create a perverse incentive for companies: so long as enough data breaches take place, individual companies will never be found liable.").

As for damages, Defendants' negligence caused each class member cognizable injury: the market value of the hacker's unauthorized access to the PII (as to Capital One and AWS) and the cost of access to ongoing identity theft and fraud monitoring (as to Capital One and AWS). As discussed above in Section IV.A.1, these damages methodologies focus on mechanistic calculation using class-wide data and do not preclude a finding of predominance.

4. Predominance is satisfied as to Plaintiffs' statutory claims.

Plaintiffs' claims on behalf of the respective state subclasses for violations of California's UCL and CLRA, Florida's DUTPA, New York's GBL, and Washington's CPA, should also be certified. As explained above, all class members provided their PII to Capital One and all suffered the theft of that PII in the Breach, and thus, whether Defendants' inadequate data security and/or uniform misrepresentations or omissions regarding that data security violated these statutes is a common, predominating question that will be answered the same way for each class member.

Likewise, whether class members' harm was caused by Defendants' misrepresentations or omissions regarding the adequacy of their data security can be proved class-wide because class members are entitled to a presumption of reliance on uniform misrepresentations or failures to disclose material information. *See In re Arris Cable Modem Consumer Litig.*, 327 F.R.D. 334, 364-65 (N.D. Cal. 2018) (class members in CLRA and UCL actions "are not required to prove their individual reliance on the allegedly misleading statements. Instead, the standard in actions under both the CLRA and UCL is whether members of the public are likely to be deceived," making such claims "ideal for class certification because they will not require the court to

investigate class members' individual interaction with the product") (internal quotations omitted); Doc. 879 at 63-64 ("The FDUTPA does not require that a plaintiff prove the consumer actually relied on the deceptive or unfair practice. . . . Instead, a plaintiff need only provide that 'the alleged practice was likely to deceive a consumer acting reasonably in the same circumstances.'") (quoting *Cold Stone Creamery, Inc. v. Lenora Foods I, LLC*, 332 F. App'x 565, 567 (11th Cir. 2009)); *Hasemann v. Gerber Prod. Co.*, 331 F.R.D. 239, 257 (E.D.N.Y. 2019) (the GBL "does not require proof that a consumer actually relied on the misrepresentation"); *Davidson v. Apple, Inc.*, 2018 WL 2325426, at *16 (N.D. Cal. May 8, 2018) ("[F]ederal and state cases interpreting the WCPA have found that there is [] a rebuttable presumption of reliance for WCPA fraud claims. This presumption also renders causation unproblematic because in omissions cases the presumption of reliance resolves causation problems . . . .") (internal quotations and citations omitted).

In addition, courts routinely conclude that the practice of maintaining deficient data security for customer PII itself violates unfair business practices statutes without regard to any misrepresentations or omissions. *See In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1226-27 (N.D. Cal. 2014) (maintaining deficient data security violates the UCL's unlawful and unfair prongs); *Burrows v. Purchasing Power, LLC*, 2012 WL 9391827, at *6 (S.D. Fla. Oct. 18, 2012) (allegation "that Defendants failed to adequately secure his PII[] qualifies as an unfair practice" under the FDUTPA); *Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1162 (W.D. Wash. 2017) (failure to maintain adequate data security is unfair business practice under the WCPA).

Plaintiffs' claims for Defendants' violations of these statutes and the damages caused therefrom can be proven with common evidence of Defendants' inadequate data security and

common misrepresentations and omissions regarding the adequacy of their data security, and therefore, predominance is satisfied as to these claims.

B. Superiority Is Satisfied.

Superiority under Rule 23(b)(3) requires that use of a class action be "superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3). Factors the district court should consider include: "(A) the class members' interest in individually controlling the prosecution or defense of separate actions; (B) the extent and nature of any litigation concerning the controversy already begun by or against class members; (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (D) the likely difficulties in managing the class action." Fed. R. Civ. P. 23(b)(3)(A)-(D). Superiority is satisfied here.

First, the vast majority of class members have minimal interest in individually controlling the prosecution of their claims because the monetary value of their damages is "dramatically outweighed by the cost of litigating an individual case." *See In re TD Bank*, 325 F.R.D. at 162 (citing Fed. R. Civ. P. 23(b)(3)(A)). "Here, as in many consumer protection lawsuits, 'the low amount of . . . damages available means no big . . . damages award on the horizon, thus making an individual action unattractive from a plaintiff's perspective.'" *Id.* (quoting *Stillmock v. Weis Markets, Inc.*, 385 F. App'x 267, 274 (4th Cir. 2010)) (alternations in original). "In other words, for most class members the only realistic alternative to a class action is no action at all." *Id.* Conversely, "[i]f any individual class member does wish to retain control of his claim, or seek actual damages where a different remedy might be imposed upon him, the opt-out mechanism will allay such a presumption upon his individual interests." *Id.*

Second, "numerous putative class action lawsuits based on the same facts and containing substantively identical claims have already been filed against" Defendants, and the Judicial Panel

on Multidistrict Litigation concluded it was appropriate to consolidate the handling of those common claims in this Court, "which favors a consolidated disposition generally." *Id.* (citing Fed. R. Civ. P. 23(b)(3)(B)); *see also* Fed. R. Civ. P. 23(b)(3)(C).

Third, "the difficulties that would necessarily be presented by thousands upon thousands of individual actions far outweigh any difficulties the Court may encounter in managing a class action in this case." *Id.* (citing Fed. R. Civ. P. 23(b)(3)(D)). "Put simply, '[a] class action is the only realistic way Plaintiffs' claims can be adjudicated. Separate actions by each of the class members would be repetitive, wasteful, and an extraordinary burden on the courts.'" *Id.* (quoting *In re Checking Account Overdraft Litig.*, 286 F.R.D. at 659)). Superiority is satisfied here.

V. THE COURT SHOULD CERTIFY A RULE 23(b)(2) CLASS FOR DECLARATORY RELIEF.

Certification of a claim for declaratory relief is appropriate when, in addition to the four requirements of Rule 23(a) discussed above, "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief . . . is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). "When a class seeks an indivisible injunction benefiting all its members at once, there is no reason to undertake a case-specific inquiry into whether class issues predominate or whether class action is a superior method of adjudicating the dispute." *Dukes*, 564 U.S. at 362-63. Accordingly, the "key to the (b)(2) class is 'the indivisible nature of the injunctive or declaratory remedy warranted—the notion that the conduct is such that it can be enjoined or declared unlawful only as to all of the class members or as to none of them.'" *Id.* at 360 (quoting Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. REV. 97, 132 (2009)).

"[T]here is no *per se* rule prohibiting class certification under Rule 23(b)(2) when monetary damages are sought." *Olvera-Morales v. Intern. Labor Mgmt. Corp.*, 246 F.R.D. 250, 259

(M.D.N.C. 2007); *see also Thorn v. Jefferson-Pilot Life Ins. Co*., 445 F.3d 311, 331-32 (4th Cir. 2006) ("[W]e do not hold, nor have we ever held, that monetary relief is fundamentally incompatible with Rule 23(b)(2)."). "Rather, the Fourth Circuit has held 'only that relief that is neither injunctive nor declaratory may not predominate over the injunctive and declaratory relief in a proper Rule 23(b)(2) action.'" *Olvera-Morales*, 246 F.R.D. at 259 (quoting *Thorn*, 445 F.3d at 331). As explained above, Plaintiffs' monetary related certification requests are all sought under Rule 23(b)(3), and thus the line of Fourth Circuit cases related to whether such monetary damages are "incidental" to the request for injunctive or declaratory relief under Rule 23(b)(2) is inapposite.[24] Plaintiffs' requested 23(b)(2) relief is injunctive and declaratory only.

Here, Plaintiffs' declaratory relief claim meets the Rule 23(b)(2) standard because Defendants acted in a manner common to the class. Defendants subjected all class members' PII to the same security vulnerabilities; class members' PII was compromised as a result of those vulnerabilities; Defendants are still in possession of class members' PII; and Defendants still have not adequately secured the PII.[25] A declaration of such is appropriate and injunctive relief is thus needed to remediate Defendants' inadequate security, which uniformly applies to all class members. Plaintiffs' expert Professor Madnick has set forth the inadequacies in Defendants'

---

[24] *See, e.g.*, *Fisher v. Virginia Elec. & Power Co*., 217 F.R.D. 201, 213 (E.D. Va. 2003) ("Nevertheless, Rule 23(b)(2) certification remains available when a claim for injunctive or declaratory relief *also includes* a claim for money damages so long as the requested damages are 'incidental' to the requested injunctive or declaratory relief. Incidental damages are those that flow directly from liability to the class as a whole on the claims that form the basis of the injunctive or declaratory relief. Such damages are distinguishable in that they do not depend in any significant way on the intangible, subjective differences of each class member's circumstances and do not require additional hearings to resolve the disparate merits of each individual's case.") (emphasis added) (internal citations and quotation marks omitted); *Olvera-Morales*, 246 F.R.D. at 258 (same).

[25] Injunctive relief is also available and can be resolved on a class-wide basis for the respective classes' claims under the UCL (Cal. Bus. & Prof. § 17204), CLRA (Cal. Civ. Code § 1780(a)), FDUTPA (Fla. Stat. Ann. § 501.211(1)), and WCPA (Wash. Rev. Code Ann. § 19.86.090).

proposed remediations and the security controls needed to protect class members' PII now and in the future. These include:

- Ensuring that all breached data has been discovered and destroyed to prevent further endangering Plaintiffs in the future;
- Deleting all PII from the systems that do not serve a clear, critical, permissible, and authorized business purpose;
- Maintaining a consistent and continuous effort to search for the breached data on dark web marketplaces and seek its destruction when located;
- Continuous and periodic independent expert review, with reports to the Court and to Plaintiffs;
- Sharing of threat and vulnerability information that AWS gathers from its threat intelligence, honeypots, and other activities with Capital One.

Ex. 4, Madnick at 27-32.

Given Defendants' uniform ongoing treatment of the PII at issue, this is an ideal case for certification of claims for declaratory and injunctive relief under Rule 23(b)(2). *See Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 697-99 (N.D. Cal. 2019) (certifying Rule 23(b)(2) class seeking declaration of insufficient data security practices and corresponding injunctive relief).

VI. ALTERNATIVELY, THE COURT SHOULD GRANT ISSUE CERTIFICATION UNDER RULE 23(c)(4).

Certification of particular issues is proper pursuant to the express language of Rule 23(c)(4), if necessary. In *Good v. American Water Works Co., Inc*., the court stated, "[t]here is no impediment to certifying particular issues in a case as opposed to entire claims or defenses. That is the very approach urged by the authoritative Manual for Complex Litigation." 310 F.R.D. 274, 296 (S.D. W. Va. 2015). "Rule 23(c)(4)(A) permits a class to be certified for *specific issues or elements of claims* raised in the litigation." *Id.* (quoting Manual for Complex Litigation, § 21.24 (4th 2004)) (emphasis in original). "An issues-class approach contemplates a bifurcated trial where the common issues are tried first, followed by individual trials on questions such as proximate

causation and damages." *Id*. (quoting Manual for Comp. Litig.). "If otherwise compliant with Rule 23, the proposed liability issue certifications provide an orderly means to resolve some of the central issues in the case. That is an approach that is encouraged by our court of appeals." *Id*. (citing *In re A.H. Robins*, 880 F.2d 709, 740 (4th Cir. 1989)).

Thus, in *Good*, a pollution case, the court held that, "the proposed liability issue certification is appropriate under Rule 23(c)(4)." 310 F.R.D. at 296. "Absent the proposed liability issues certification, the issue of fault, for one, would have to be tried seriatim in every case for which a jury is empaneled." *Id*. at 297. Likewise, if necessary, this Court should certify issues-based classes—e.g., for duty and breach as to both negligence and contract claims—rather than denying Plaintiffs' motion for class certification entirely. In the event of a liability determination under Rule 23(c)(4), class members who suffered damages such as out-of-pocket losses from fraud, the value of time spent dealing with the breach, and mitigation expenses could individually pursue those damages. *See, e.g.*, *Kay Co., LLC v. EQT Prod. Co.*, 2017 WL 10436074, at *16 (N.D. W. Va. Sept. 6, 2017) ("Rule 23(c)(4) permits courts to certify a class with respect to particular issues and contemplates possible class adjudication of liability issues with 'the members of the class . . . thereafter . . . required to come in individually and prove the amounts of their respective claims."). Absent a class-wide determination of the issues most burdensome to prove in terms of time, experts, and Court resources, wronged consumers may be left with no practicable route to a remedy. *Cf. Pella Corp. v. Saltzman*, 606 F.3d 391, 394 (7th Cir. 2010) (resolution of common liability questions "has the potential to eliminate the need for multiple, potentially expensive expert testimony and proof that would cost considerably more to litigate than the claims would be worth to the plaintiffs").

CONCLUSION

For the foregoing reasons, Plaintiffs' Motion for Class Certification should be granted.

DATED: April 28, 2021

Respectfully Submitted,

/s/ *Steven T. Webster*

Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
swebster@websterbook.com

Plaintiffs' Local Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN, P.L.L.P
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Plaintiffs' Lead Counsel